Department of Defense

INSTRUCTION

NUMBER 5215.2

September 2, 1986

ASD(C3I)

SUBJECT: Computer Security Technical Vulnerability Reporting Program (CSTVRP)

References: (a) National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security," September 17, 1984

(b) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972

(c) DoD Directive 5215.1, "Computer Security Evaluation Center," October 25, 1982

(d) through (f) see enclosure E1.

1. PURPOSE

This Instruction:

1.1. Establishes a Computer Security Technical Vulnerability Reporting Program (CSTVRP) under the direction of the National Security Agency, National Information Security Assessment Center (NISAC), reference (a).

1.2. Establishes procedures for reporting all demonstrable and repeatable technical vulnerabilities of Automated Information Systems (AIS).

1.3. Provides for the collection, consolidation, analysis, reporting or notification of generic technical vulnerabilities and corrective measures in support of the DoD Computer Security requirements in reference (b).

1.4. Establishes methodologies for dissemination of vulnerability information.

2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and Defense Agencies (hereafter referred to collectively as "Components").

2.2. The program shall be focused on technical vulnerabilities in commercially available hardware, firmware and software products acquired by Department of Defense and those altered commercial products supporting standard military applications. Research prototypes and reproduction commercial products are excluded from the program. Correction of site-specific vulnerabilities are primarily the responsibility of the affected Component.

2.3. These reporting procedures are in addition to any existing reporting requirements on technical AIS vulnerabilities. Copies of reports prepared in accordance with existing reporting requirements may be provided to satisfy the requirements of Section 6 and Enclosure E2.

2.4. The reporting portion of the program is also available on a voluntary basis for the non-DoD AIS community.

3. DEFINITIONS

The following definitions are applicable for this Instruction:

3.1. AIS Resource Manager: The individual with direct operational control of the AIS hardware, firmware, and/or software, or individuals who are in a position to identify and report the technical vulnerability.

3.2. Automated Information System (AIS): A system which creates, prepares or manipulates information in electronic form and includes computers, word processing systems and other electronic information handling systems and associated equipment (reference (c)).

3.3. Evaluated Products List (EPL): A documented inventory of equipment and hardware, software or firmware systems that have been evaluated against and certified to be technically compliant with the Department of Defense Trusted Computer System Evaluation Criteria (reference (d)) by the National Computer Security Center (NCSC) (reference (c)).

3.4. Focal Point: The computer security contact within the OSD Components, Military Departments, the Organization of the Joint Chiefs of Staff, Unified and Specified Commands, Defense Agencies, the intelligence community, and other Government organizations involved in the processing of sensitive or classified information.

3.5. Technical Vulnerability: A hardware, firmware, or software weakness or design deficiency that leaves an automated information system open to potential exploitation either externally or internally, thereby resulting in risk or compromise of information, alteration of information, or denial of service. Technical vulnerability information, if made available to unauthorized persons, may allow an AIS to be exploited, resulting in potentially serious damage to national security.

4. POLICY

It is DoD policy that:

4.1. All DoD Components shall contribute to the NISAC, through their Focal Points, information concerning technical vulnerabilities. This will constitute a technical reporting channel for the purposes of the CSTVRP.

4.2. The NISAC shall maintain a central repository of computer vulnerability information.

4.3. Information on the technical vulnerabilities of AIS's shall be protected from unauthorized disclosure while ensuring it is disseminated to individuals responsible for the security of an AIS.

4.4. Generic vulnerability information may be released to support DoD AIS acquisition processes.

4.5. Technical vulnerabilities will be evaluated on a case-by-case basis on behalf of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) to determine the extent of their impact.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)) has staff supervision and shall oversee and review

implementation of this Instruction.

5.2. The Heads of DoD Components shall:

5.2.1. Appoint a Focal Point to ensure the execution of the responsibilities and procedures specified.

5.2.2. Develop procedures for the reporting of technical vulnerabilities, establish classification guidance for national security information (reference (e)), and establish procedures for the dissemination and protection of technical vulnerability information consistent with forms and guidance developed by the NISAC and in accordance with reference (e).

5.3. The National Information Security Assessment Center shall be responsible for implementing and maintaining a CSTVRP. The NISAC shall:

5.3.1. Review reported vulnerabilities to assess the possible impact within the Department of Defense and to evaluate the requirement for and extent of further dissemination.

5.3.2. Act as the clearinghouse for all DoD AIS technical vulnerability information, collecting it from and disseminating it to the Component Focal Points.

5.3.3. Establish procedures to encourage the voluntary submission of technical vulnerability information from non-DoD Automated Information System users.

5.3.4. Establish and maintain a data base of technical vulnerability information having security commensurate with its sensitivity.

5.3.5. Establish procedures for transmitting technical vulnerability information to affected manufacturers for corrective action.

5.3.6. Collect, analyze, catalogue and disseminate vulnerability information from periodicals, newspaper articles, trade papers, research papers, field research, etc.

5.4. The National Computer Security Center shall:

5.4.1. Perform technical analysis of computer security vulnerabilities on a case-by-case basis.

5.4.2. Evaluate reported computer security technical vulnerabilities in products on the EPL to determine the impact on the products trusted system rating.

5.5. The DoD Component Focal Points shall:

5.5.1. Receive technical vulnerability reports and information from their AIS Resource Managers in accordance with the procedures of section 6, below.

5.5.2. Review and analyze the vulnerability report. In conformance with DoDD 5200.28, assess the impact of the vulnerability on system accreditation, and assess potential technical solutions.

5.5.3. Report technical vulnerabilities and potential solutions to the NISAC under the procedures stated in section 6, below.

5.5.4. Disseminate technical vulnerability reports within the Component, on a valid need-to-know basis, receive and process all Component requests for vulnerability information, and, when necessary, request additional information from the NISAC.

5.5.5. The Component Focal Point will, in coordination with the Designated Approving Authority (DAA), implement a course of action to reduce the risk, pending a detailed technical evaluation of the vulnerability by the NCSC, in conformance with DoDD 5200.28.

5.6. The AIS Resource Manager shall:

5.6.1. Report identified vulnerabilities to the respective Agency Focal Point in accordance with enclosure E2.

5.6.2. Recognize that compliance with this Instruction does not preclude the responsibility to take any necessary and prudent action to reduce all risk presented by the vulnerability.

6. PROCEDURES

6.1. Technical vulnerabilities shall be reported by the responsible AIS Resource Manager to the cognizant Focal Point in accordance with procedures established by the Focal Point for the organization. Reports of technical vulnerabilities should be in

sufficient detail so the vulnerability can be demonstrated and repeated (enclosure E2.).

6.2. The Component Focal Point shall ensure that the reported vulnerability is screened for technical validity and determine to the best of available capabilities the extent of risk presented by the technical vulnerability to the operation of the activity or other activities.

6.3. The Component Focal Point shall, within four weeks of receipt of a valid vulnerability, forward a copy of the report to the NISAC with a summary of the reported vulnerability, the analysis of the risk involved, and any recommended solutions to correct the vulnerability commensurate with established Component programs. This summary shall be in narrative form in accordance with enclosure E2. and shall be transmitted in accordance with reference (e). The outer envelope will be addressed to:

National Security Agency
Ft. George G. Meade, MD 20755-6000
ATTN: Chief, S2

The inner envelope will be marked:

ATTN CSTVRP/S2093

Vulnerability reports requiring transmission via the Armed Forces Courier Service will be addressed to:

National Security Agency
Ft. George G. Meade
ATTN: S2

6.4. Technical vulnerabilities in products on the NCSC Evaluated Product List shall be reported by the Component Focal Point to the NISAC within two days of receipt. A follow-up report will be submitted in conformance with subsection 6.3 above. The NCSC will evaluate the risk to the EPL item and make a specific determination as to whether or not to retain, reduce, or rescind its current trusted system rating.

6.5. While the intent of the CSTVRP is not to task the NISAC with correcting reported technical vulnerabilities, the NISAC may use such resources as are available

to resolve any vulnerabilities forwarded by the Component Focal Points. The NISAC may request that the responsible vendor correct the vulnerability. Any technical vulnerabilities in products appearing on the EPL will be referred to the responsible vendor for correction. Appropriate warnings will be disseminated.

6.6. The NISAC shall maintain the technical vulnerability data base for DoD. DoD activities may request information from this data base through their Component Focal Points. The Focal Point must verify the activity's clearance and need to know.

6.7. Dissemination of Technical Vulnerability Information:

6.7.1. Technical vulnerability information will be disseminated by the NISAC to the Component Focal Points. Technical vulnerabilities affecting more than one Component, as identified by the Automated Resource Management System (ARMS) or equivalent systems, shall be disseminated by the NISAC to the appropriate Component Focal Points, consistent with dissemination protection policies.

6.7.2. The Component Focal Point shall disseminate information about valid vulnerabilities to activities within its own Component. The Component Focal Point will ensure that dissemination is strictly limited to those activities and individuals with necessary clearance and a valid need to know.

6.8. Protection and Handling of Vulnerability Information:

6.8.1. A technical vulnerability reported under this Instruction from DoD sources shall be classified at least CONFIDENTIAL. It may be classified higher if so determined by the original classification authority.

6.8.2. A technical vulnerability reported under this Instruction from non-DoD sources within the Federal Government and/or from non-government sources shall be classified at least CONFIDENTIAL. It may be classified higher if so determined by the original classification authority. If there is no authority to classify or to handle classified information, a vulnerability report shall be marked as unclassified sensitive national security related information. Such a report shall be protected from public disclosure in accordance with applicable statutes, directives, executive orders and regulations.

6.8.3. Vendors may be provided the technical details of reported vulnerabilities to make corrections, but shall not be provided information about the specific site(s) concerned, methods of discovery, or other information which could lead to increased site vulnerability without the express written approval of the Head of the

DoD Component or the DAA. Release of this information will be approved on a case-by-case basis and in accordance with this Instruction and appropriate Directives.

7. INFORMATION REQUIREMENTS

The procedures described in section 6 have been assigned Report Control Symbol NSA/CSS-1057.

8. EFFECTIVE DATE AND IMPLEMENTATION

This Instruction is effective immediately. Forward one copy of implementing documents to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) within 120 days.

Donald C. Latham
Assistant Secretary of Defense
(Command, Control, Communications
and Intelligence)

Enclosures - 3

1. References, continued
2. Reporting Format
3. Vulnerability Report Sample

E1. ENCLOSURE 1

REFERENCES, continued

(d) DoD 5200.28 STD, Department of Defense Standard, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985

(e) DoD Regulation 5200.1-R, "DoD Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, June 7, 1982.

(f) DoD Directive 5230.24, "Distribution Statements on Technical Documents," November 20, 1984.

E2. ENCLOSURE 2

REPORTING FORMAT

The following format should be used for reporting technical vulnerabilities. A format example with sample data is attached to this reporting format.

Vulnerability Report

Classification markings/Distribution statements

A. Required Information

1. Report Date

2. Contact

a. Name

b. Organization

c. Mailing address

d. Phone number

e. Position

3. Hardware/Software

a. List hardware and system configuration

b. Software description

(1) Operating system (include release number).

(2) Describe any unique attributes - i.e., locally modified special security properties.

B. Executive Summary of Vulnerability.

A description of the nature and effect of the vulnerability in as general terms

as possible.

C. Description of Technical Vulnerability.

1. A scenario that describes specific conditions to demonstrate the weakness or design deficiency. The description should sufficiently describe the conditions so that the weakness or design deficiency can be repeated without further information. This scenario may include source or object code.

2. Describe the specific impact or effect of the weakness or design deficiency in terms of the following: (1) denial of service, (2) alteration of information, and/or (3) compromising of data. Cite specific examples as appropriate.

3. Indicate whether or not the affected vendor has been notified.

D. Suggested Fixes.

- Describe any code or procedures you may have discovered that when implemented may reduce the impact of the defined technical vulnerability.

E. Additional Information.

1. System Specifics

a. Location

b. Owner

c. Network connections

d. Security attributes

2. System use and highest classification of data on system.

3. Additional clarifying information.

E3. ENCLOSURE 3

VULNERABILITY REPORT

Classification Marking/Distribution statement

A. 1. YYMMDD

2. a. Dave Bowman, Lt. Col., USAF

b. U.S. Space Command (USSPACECOM)

c. Colorado Springs, CO 11111-1111

d. AV 111-1111, com (303) JCN-6325

e. Senior Astronaut

3. a. HAL 9000

512 GB memory

2 360 MB fixed head disk drives

1 card reader

45 teleprinters

1 lineprinter

b. (1) Clarke, Version 20.10

(2) Locally modified to increase positive auditing.

B. The Clarke version 20.10 operating system permits one process to gain unauthorized access to the data area of another process. This flaw could allow a user to gain full access to any data on the system.

C. 1. Assume two coordinating processes. Process 1 attempts to access a piece of data it has full access rights to. In doing this, process 1 is causing access attributes (data area, name of user attempting the access) to be passed to a procedure

"check-access."

The procedure check-access takes the attributes, makes appropriate comparisons, and finds that process 1 has full access to the data. Before check-access completes execution and returns, process 2 gains the attention of the CPU (using priority interrupts).

While process 2 is executing it overwrites an area in process 1. This area was the location in which process 1 had stored the name of the data area it was attempting to access (a parameter). This caused the data area that the procedure check-access was using to determine process 1's access rights to be overwritten.

Process 2 then terminates its own execution and allows process 1 to resume. Since check-access granted access to process 1 for the original data area, check-access will inform process 1 that it is allowed access to a data area other than the one that was originally in question.

The reasons for this problem are:

(1) Process 2 was allowed to interrupt check-access without causing a reverification of the input parameters.

(2) input parameters were allowed to remain in user space between the time the parameters were checked and the time the parameters were sent back to the calling procedure.

2. This design deficiency allows a user process to gain full access to any data on the system. Since no change is made to existing access rules, there is no evidence that the unauthorized use took place. The audit log will only pick up this access if positive auditing is taking place.

3. The vendor, Highorder Artificial Reasoning, Deduction, and Intelligence Engineering Corp., has been informed and is currently preparing a fix to be distributed as soon as possible.

D. One remedy to this problem would have check-access (as well as some other procedures) copy input parameters into system space before using them. This would prevent processes from changing parameters during a system procedure call.

E. 1. a. U.S. Space Command Computer Operations Center Colorado Springs, CO.

b. U. S. Space Command.

c. Defense Data Network (DDN), MILNET.

d. "GUARD DOG" commercial security software package for HAL 9000 installed. Remote user access is mediated through use of passwords and "CALL GUARD" call-back devices.

2. System operates in System High security mode. Highest classification of data on system is SECRET.

3. System is available through the MILNET to researchers at fifteen universities and research institutes.